THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appellant(s):	Brian J. Reistad et al.
Appl. No.:	09/054,180
Conf. No.:	2217
Filed:	April 1, 1998
Title:	ELECTRONIC COMMERCE SYSTEM
Art Unit:	3621
Examiner:	Firmin Backer
Docket No.:	0115274-0008

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

SUPPLEMENTAL APPEAL BRIEF

Sir:

Appellants submit the present Supplemental Appeal Brief in response to the Notice of Non-Compliant Appeal Brief dated March 14, 2007. The notice required Appellant to "summarize each independent claim separately" and provide a concise explanation of the subject matter. Appellants respectfully submit that this requirement was met in the original Appeal Brief (see pages 6-7). Nevertheless, in the interests of progressing the present appeal, Appellants have re-formatted the description of the claimed subject matter in an earnest effort to comply with the examiner's request.

This brief is filed in support of the Notice of Appeal filed on September 14, 2006. This Appeal is taken from the Final Rejection in the Office Action dated June 14, 2006, and Notice of Panel Decision from Pre-Appeal Brief Review dated November 16, 2006. For brevity's sake, copies of exhibits that were previously submitted will not be attached to this document.

I. REAL PARTY IN INTEREST

The real party in interest for the above-identified patent application on Appeal is Soverain Software LLC by virtue of an Assignment dated June 26, 2003 and recorded at reel 015083, frame 0204 in the United States Patent and Trademark Office.

II. RELATED APPEALS AND INTERFERENCES

Appellants' legal representative and the Assignee of the above-identified patent application do not know of any prior or pending appeals, interferences or judicial proceedings which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision with respect to the above-identified Appeal.

III. STATUS OF CLAIMS

Claims 12-36 and 39-63 are pending in the above-identified patent application. Claims 12-36 and 39-63 have been rejected. Claims 12-36 and 39-63 are being appealed in this Brief. A copy of the appealed claims is included in the Claims Appendix.

IV. STATUS OF AMENDMENTS

A Final Office Action was mailed on June 14, 2006. Appellants filed a Notice of Appeal in Response on September 14, 2006. A copy of the Final Office Action is attached as Exhibit A in the Evidence Appendix.

V. SUMMARY OF CLAIMED SUBJECT MATTER

A summary of the invention by way of reference to the drawings and specification for each of the independent claims is provided as follows:

Independent claims 12 and 39 are directed to a client computer (12) being programmed to transmit to a server computer (14), over a public packet-switched network (FIG. 1), an order acceptance request (16) comprising a plurality of terms or conditions of a proposed offer for a purchase (specification page 1, lines 1-27). The order acceptance request comprises a discrete message that includes a plurality of modular elements (page 1, lines 1-17) whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements (page 9, lines 20-29). At least one of the modular elements individually protected by a cryptographic security code is a digital coupon (page 9, lines 29-32)

A server computer processes the order acceptance request (16) (page 5, lines 19-30) based on pre-programmed criteria, including authentication of the cryptographic security codes embedded within each of the modular elements (page 9, lines 6-29) and examination of the modular elements of the discrete message individually protected by the cryptographic security codes (page 5, line 18 - page 6, line 2), and, based on the processing of the order acceptance request (16), to transmit to the client computer an order acceptance response (18) based on the pre-programmed criteria (page 6, lines 3-24). The order acceptance response (18) comprises a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements (page 15, lines 16-25) whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements (page 10, lines 3-8; page 5, line 18 - page 6, line 2; page 21, lines 13-16). The client computer is programmed to receive the digital coupon, protected by a cryptographic security code, from another computer (page 9, lines 29-32).

Independent claims 13 and 40 are directed to a client computer (12) being programmed to transmit to a server computer (14), over a public packet-switched network (FIG. 1), an order acceptance request (16) comprising a plurality of terms or conditions of a proposed offer for a purchase (specification page 1, lines 1-27). The order acceptance request comprises a discrete message that includes a plurality of modular elements (page 1, lines 1-17) whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements (page 9, lines 20-29). At least one of the modular elements individually protected by a cryptographic security code is a digital coupon (page 9, lines 29-32)

A server computer processes the order acceptance request (16) (page 5, lines 19-30) based on pre-programmed criteria, including authentication of the cryptographic security codes embedded within each of the modular elements (page 9, lines 6-29) and examination of the modular elements of the discrete message individually protected by the cryptographic security codes (page 5, line 18 - page 6, line 2), and, based on the processing of the order acceptance request (16), to transmit to the client computer an order acceptance response (18) based on the pre-programmed criteria (page 6, lines 3-24). The order acceptance response (18) comprises a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements (page 15, lines 16-25) whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements (page 10, lines 3-8; page 5, line 18 - page 6, line 2; page 21, lines 13-16). The digital coupon is configured to be used by any coupon holder that possesses the digital coupon, and wherein the server computer is programmed to accept the digital coupon without regard to the identity of the coupon holder (page 19, lines 9-16).

Independent claims 14 and 41 are directed to a client computer (12) being programmed to transmit to a server computer (14), over a public packet-switched network (FIG. 1), an order acceptance request (16) comprising a plurality of terms or conditions of a proposed offer for a purchase (specification page 1, lines 1-27). The order acceptance request comprises a discrete message that includes a plurality of modular elements (page 1, lines 1-17) whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements (page 9, lines 20-29). At least one of the modular elements individually protected by a cryptographic security code is a digital coupon (page 9, lines 29-32)

A server computer processes the order acceptance request (16) (page 5, lines 19-30) based on pre-programmed criteria, including authentication of the cryptographic security codes embedded within each of the modular elements (page 9, lines 6-29) and examination of the modular elements of the discrete message individually protected by the cryptographic security codes (page 5, line 18 - page 6, line 2), and, based on the processing of the order acceptance request (16), to transmit to the client computer an order acceptance response (18) based on the pre-programmed criteria (page 6, lines 3-24). The order acceptance response (18) comprises a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements (page 15, lines 16-25) whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements (page 10, lines 3-8; page 5, line 18 - page 6, line 2; page 21, lines 13-16). The server computer is programmed to determine whether a coupon holder is authorized to use the digital coupon and to accept the digital coupon only if the coupon holder is authorized to use the digital coupon (page 19, lines 16-29).

Independent claims 34 and 61 are directed to a client computer (12) being programmed to transmit to a server computer (14), over a public packet-switched network (FIG. 1), an order acceptance request (16) comprising a plurality of terms or conditions of a proposed offer for a purchase (specification page 1, lines 1-27). The order acceptance request comprises a discrete message that includes a plurality of modular elements (page 1, lines 1-17) whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements (page 9, lines 20-29). At least one of the modular elements individually protected by a cryptographic security code is a digital coupon (page 9, lines 29-32)

A server computer processes the order acceptance request (16) (page 5, lines 19-30) based on pre-programmed criteria, including authentication of the cryptographic security codes embedded within each of the modular elements (page 9, lines 6-29) and examination of the modular elements of the discrete message individually protected by the cryptographic security codes (page 5, line 18 - page 6, line 2), and, based on the processing of the order acceptance request (16), to transmit to the client computer an order acceptance response (18) based on the pre-programmed criteria (page 6, lines 3-24). The order acceptance response (18) comprises a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements (page 15, lines 16-25) whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements (page 10, lines 3-8; page 5, line 18 - page 6, line 2; page 21, lines13-16). The cryptographic security codes are embedded within respective ones of the plurality of modular elements (page 9, lines 20-23).

Independent claims 35 and 62 are directed to a client computer (12) being programmed to transmit to a server computer (14), over a public packet-switched network (FIG. 1), an order acceptance request (16) comprising a plurality of terms or conditions of a proposed offer for a purchase (specification page 1, lines 1-27). The order acceptance request comprises a discrete message that includes a plurality of modular elements (page 1, lines 1-17) whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements (page 9, lines 20-29). At least one of the modular elements individually protected by a cryptographic security code is a digital coupon (page 9, lines 29-32)

A server computer processes the order acceptance request (16) (page 5, lines 19-30) based on pre-programmed criteria, including authentication of the cryptographic security codes embedded within each of the modular elements (page 9, lines 6-29) and examination of the modular elements of the discrete message individually protected by the cryptographic security codes (page 5, line 18 - page 6, line 2), and, based on the processing of the order acceptance request (16), to transmit to the client computer an order acceptance response (18) based on the pre-programmed criteria (page 6, lines 3-24). The order acceptance response (18) comprises a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements (page 15, lines 16-25) whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements (page 10, lines 3-8; page 5, line 18 - page 6, line 2; page 21, lines13-16).

Independent claims 36 and 63 are directed to a client computer (12) being programmed to transmit to a server computer (14), over a public packet-switched network (FIG. 1), an order acceptance request (16) comprising a plurality of terms or conditions of a proposed offer for a purchase (specification page 1, lines 1-27). The order acceptance request comprises a discrete message that includes a plurality of modular elements (page 1, lines 1-17) whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements (page 9, lines 20-29). At least one of the modular elements individually protected by a cryptographic security code is a digital coupon (page 9, lines 29-32). The cryptographic security codes are digital signatures (page 9, lines 24-25).

A server computer processes the order acceptance request (16) (page 5, lines 19-30) based on pre-programmed criteria, including authentication of the cryptographic security codes embedded within each of the modular elements (page 9, lines 6-29) and examination of the modular elements of the discrete message individually protected by the cryptographic security codes (page 5, line 18 - page 6, line 2), and, based on the processing of the order acceptance request (16), to transmit to the client computer an order acceptance response (18) based on the pre-programmed criteria (page 6, lines 3-24). The order acceptance response (18) comprises a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements (page 15, lines 16-25) whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements (page 10, lines 3-8; page 5, line 18 - page 6, line 2; page 21, lines13-16).

Dependent claims 15-33 and 42-60 depend directly and indirectly to independent claims 14 and 41, respectively. Applicant acknowledges that reference to "claim 3" in claims 19-20 and 22-23 is incorrect, since these claims were previously cancelled. "Claim 3" should be changed to "claim 14," and applicant will submit the correcting amendments at the conclusion of this appeal.

Dependent claims 15 and 42 recite the above configuration and additionally recite that the client computer is programmed to provide information to the server computer concerning the identity of the coupon holder (page 9, lines 6-20).

Dependent claims 16 and 43 recite the above configuration and additionally recite that the server computer is programmed to authenticate authority of the client computer by virtue of a two-way-authenticated SSL connection (page 9, lines 9-13).

Dependent claims 17 and 44 recite the above configuration and additionally recite that the server computer is programmed to authenticate authority of the client computer using a basic authentication method (page 9, lines 23-26).

Dependent claims 18 and 45 recite the above configuration and additionally recite that the server computer is programmed to authenticate authority of the client computer using a client certificate (page 9, lines 13-14).

Dependent claims 19 and 46 recite the above configuration and additionally recite that the digital coupon contains a serial number to ensure that the digital coupon is used only once and the server computer is programmed to determine whether the digital coupon has been used previously and to accept the digital coupon only if it has not been used previously (page 19, lines 9-21).

Dependent claims 20 and 47 recite the above configuration and additionally recite that the server computer is programmed to set at least one term of the order acceptance response based on whether the digital coupon is present in the order acceptance request (page 17, lines 18-25).

Dependent claims 21 and 48 recite the above configuration and additionally recite that the at least one term of the order acceptance response is a price (page 17, lines 18-25).

Dependent claims 22 and 49 recite the above configuration and additionally recite that the server computer is programmed to set at least one term of the order acceptance response based on whether the digital coupon in the order acceptance request is a particular type of digital coupon (page 16, lines 8-19).

Dependent claims 23 and 50 recite the above configuration and additionally recite that the digital coupon is a gift certificate (page 25, line 30 - page 26, line 12).

Dependent claims 24 and 51 recite the above configuration and additionally recite that the gift certificate comprises a serial number (page 25, line 30 - page 26, line 12).

Dependent claims 25 and 52 recite the above configuration and additionally recite that the server computer is programmed to ensure that the serial number has been used only once by checking a database in which the serial number is stored (page 26, lines 13-21).

Dependent claims 26 and 53 recite the above configuration and additionally recite that the client computer is programmed to display an icon of the gift certificate and to initiate the order acceptance request after a recipient of the gift certificate clicks on the icon (page 7, line 29 - page 8, line 2; page 26, lines 13-17).

Dependent claims 27 and 54 recite the above configuration and additionally recite a merchant computer, the merchant computer (65) being programmed to respond to the recipient clicking on the icon by transmitting an order form to the client computer, the client computer being programmed to initiate the order acceptance request when the recipient fills in the order form (page 26, lines 13-33).

Dependent claims 28 and 55 recite the above configuration and additionally recite that the client computer is a first client computer programmed to receive the gift certificate from a second client computer (page 25, line 30 - page 26, line 12).

Dependent claims 29 and 56 recite the above configuration and additionally recite that the server computer is programmed to transmit the gift certificate to the second client computer, which in turn is programmed to forward the gift certificate to the first client computer (page 25, line 30 - page 26, line 12).

Dependent claims 30 and 57 recite the above configuration and additionally recite that the gift certificate comprises a serial number and the server computer is programmed to create the serial number of the gift certificate before transmitting the gift certificate to the second client computer (page 25, line 30 - page 26, line 12).

Dependent claims 31 and 58 recite the above configuration and additionally recite that the server computer is programmed to store the serial number in a database before transmitting the gift certificate to the second client computer, and is programmed, when it receives the gift certificate from the first client computer to ensure that the serial number has been used only once by checking the database in which the serial number is stored (page 25, line 30 - page 26, line 12).

Dependent claims 32 and 59 recite the above configuration and additionally recite a merchant computer programmed to transmit the gift certificate to the server computer before the server computer transmits the gift certificate to the second client computer (page 26, lines 4-29).

Dependent claims 33 and 60 recite the above configuration and additionally recite that the merchant computer is programmed to transmit the gift certificate to the server computer in the form of an order acceptance request that includes extension information indicating that the order acceptance request is a gift certificate (page 26, lines 4-29).

Although specification citations are given in accordance with C.F.R. 1.192(c), these reference numerals and citations are merely examples of where support may be found in the specification for the terms used in this section of the Brief. There is no intention to suggest in any way that the terms of the claims are limited to the examples in the specification. As demonstrated by the citations above, the claims are fully supported by the specification as required by law. However, it is improper under the law to read limitations from the specification into the claims. Pointing out specification support for the claim terminology as is done here to comply with rule 1.192(c) does not in any way limit the scope of the claims to those examples from which they find support. Nor does this exercise provide a mechanism for circumventing the law precluding reading limitations into the claims from the specification. In short, the specification citations are not to be construed as claim limitations or in any way used to limit the scope of the claims.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 12-36, and 39-63 were rejected under 35 U.S.C. §102(e) as being clearly anticipated by *Barnett et al.* (US Patent 6,321,208). A copy of the *Barnett* reference is attached hereto as Exhibit B.

VII. ARGUMENT

A. LEGAL STANDARDS

1. Anticipation under 35 U.S.C. § 102

Anticipation is a factual determination that "...requires the presence in a single prior art disclosure of each and every element of a claimed invention." *Lewmar Marine, Inc. v. Barient, Inc.*, 3 U.S.P.Q.2d 1766 (Fed. Cir. 1987). Moreover, "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a *single* prior art reference." *Verdegaal Bros. v. Union Oil of California*, 2 U.S.P.Q.2d 1051, 1053 (Fed. Cir. 1987)(*emphasis added*).

Federal Circuit decisions have repeatedly emphasized the notion that anticipation cannot be found where less than all elements of a claimed invention are set forth in a reference. *See, e.g. Transclean Corp. v. Bridgewood Services, Inc.*, 290 F.3d 1364 (Fed. Cir. 2002). In this regard, a reference disclosing "substantially the same thing" is not enough to anticipate. *Jamesbury Corp. v. Litton Indust. Prod., Inc.*, 756 F.2d 1556, 1560 (Fed. Cir. 1985). A reference must clearly disclose each and every limitation of the claimed invention before anticipation may be found.

Further, anticipation cannot be shown by combining more than one reference to show the elements of the claimed invention. *In re Saunders*, 444 F.2d 599 (C.C.P.A. 1971). All elements of a claimed invention must be disclosed in one, solitary reference. As such, it is clear that a reference cannot be utilized to render a claimed invention anticipated without identical disclosure.

B. THE CLAIMED INVENTION

The invention relates to an electronic commerce system that enables automated negotiation and processing of on-line orders. The system ensures that final orders conform to advanced order acceptability criteria established by the seller, but allows for flexibility in defining the terms and conditions of transactions to satisfy the needs of the buyer.

Client computers, such as those operated by buyers who wish to purchase goods or services from a seller, negotiate with the electronic commerce system to arrive at a set of terms and conditions which are acceptable to both the buyer and the seller. The negotiation is conducted according to a protocol which is driven by the buyer, but where the final terms and conditions must be accepted by the electronic commerce system. Once the negotiation phase is complete, when both the electronic commerce system and the client have agreed on a set of terms and conditions, the client and the electronic commerce system enter into a transaction phase wherein the terms and conditions which were agreed upon during the negotiation phase are "captured", and an order for the desired goods or services is processed according to the agreed upon terms and conditions.

During the negotiation phase the client sends an order acceptance request message to a server associated with the electronic commerce system. The order acceptance request may include data identifying the buyer, the seller, the goods or services the buyer wishes to purchase, terms and conditions of a purchasing transaction, and so forth. The server processes the order acceptance request and generates a corresponding order acceptance response which is sent back to the client. The order acceptance response includes an amended version of the original order acceptance request sent by the client. The order acceptance response identifies which of the original terms and conditions meet the server's order acceptance criteria and which do not. The order acceptance response may also identify additional required terms and conditions that may have been omitted entirely from the original request. The order acceptance response may include alternative choices that may also be acceptable to the server or a menu of proposed replacement terms, or the like.

Upon receiving the order acceptance response, the client may abandon the transaction, incorporate the server's changes into a new order acceptance request or change the order acceptance request in other ways. The client and the server continue this negotiation process until either the client abandons the negotiation or the client and the server arrive at terms and conditions acceptable to the client and which meet the order acceptance criteria of the server.

When the terms and conditions are acceptable to the client the client can enter the transaction phase by indicating client approval to the server. If the order acceptance request is acceptable to the server, the server captures the order acceptance request for the client. Capturing the order acceptance request effectively ends the negotiation between the client and the server. Backend systems associated with the electronic commerce system then process the order according to the agreed upon terms and conditions and fulfill the order.

Thus, the electronic commerce system enables automatic negotiations between a buyer and a seller, or between a client computer operating on behalf of a buyer and a server computer operating on behalf of a seller, where the server computer includes software that enforces complex order acceptance criteria. The protocol associated with the invention enables the client computer and the server computer to efficiently negotiate toward a complete and acceptable order.

According to an aspect of the invention the order acceptance request message sent from the client to the server is a discrete message that may include a plurality of modular components. The individual integrity of each modular component of the order acceptance request message is protected by a cryptographic security code embedded within the modular component. For example an order acceptance request may include a digital coupon which the client obtained from a third party, or gift certificate, or some other message component such as a free shipping offer or the like, which would impact the transaction.

When the server computer receives an order acceptance request, the server authenticates the cryptographic security codes embedded in the modular components and processes the request in accordance with the authenticated modular components. The order acceptance response message sent from the server to the client may also comprise a discrete message made up at least in part of a plurality of modular components. Again, the individual integrity of each modular component of the order acceptance response message is protected by cryptographic security codes embedded within each modular component.

Independent claims 12 and 39 are directed to a client computer (12) being programmed to transmit to a server computer (14), over a public packet-switched network (FIG. 1), an order acceptance request (16) comprising a plurality of terms or conditions of a proposed offer for a purchase (specification page 1, lines 1-27). The order acceptance request comprises a discrete message that includes a plurality of modular elements (page 1, lines 1-17) whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements (page 9, lines 20-29). At least one of the modular elements individually protected by a cryptographic security code is a digital coupon (page 9, lines 29-32)

A server computer processes the order acceptance request (16) (page 5, lines 19-30) based on pre-programmed criteria, including authentication of the cryptographic security codes embedded within each of the modular elements (page 9, lines 6-29) and examination of the modular elements of the discrete message individually protected by the cryptographic security codes (page 5, line 18 - page 6, line 2), and, based on the processing of the order acceptance request (16), to transmit to the client computer an order acceptance response (18) based on the pre-programmed criteria (page 6, lines 3-24). The order acceptance response (18) comprises a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements (page 15, lines 16-25) whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements (page 10, lines 3-8; page 5, line 18 - page 6, line 2; page 21, lines 13-16). The client computer is programmed to receive the digital coupon, protected by a cryptographic security code, from another computer (page 9, lines 29-32).

Independent claims 13 and 40 are directed to a client computer (12) being programmed to transmit to a server computer (14), over a public packet-switched network (FIG. 1), an order acceptance request (16) comprising a plurality of terms or conditions of a proposed offer for a purchase (specification page 1, lines 1-27). The order acceptance request comprises a discrete message that includes a plurality of modular elements (page 1, lines 1-17) whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements (page 9, lines 20-29). At least one of the modular elements individually protected by a cryptographic security code is a digital coupon (page 9, lines 29-32)

A server computer processes the order acceptance request (16) (page 5, lines 19-30) based on pre-programmed criteria, including authentication of the cryptographic security codes embedded within each of the modular elements (page 9, lines 6-29) and examination of the modular elements of the discrete message individually protected by the cryptographic security codes (page 5, line 18 - page 6, line 2), and, based on the processing of the order acceptance request (16), to transmit to the client computer an order acceptance response (18) based on the pre-programmed criteria (page 6, lines 3-24). The order acceptance response (18) comprises a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements (page 15, lines 16-25) whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements (page 10, lines 3-8; page 5, line 18 - page 6, line 2; page 21, lines 13-16). The digital coupon is configured to be used by any coupon holder that possesses the digital coupon, and wherein the server computer is programmed to accept the digital coupon without regard to the identity of the coupon holder (page 19, lines 9-16).

Independent claims 14 and 41 are directed to a client computer (12) being programmed to transmit to a server computer (14), over a public packet-switched network (FIG. 1), an order acceptance request (16) comprising a plurality of terms or conditions of a proposed offer for a purchase (specification page 1, lines 1-27). The order acceptance request comprises a discrete message that includes a plurality of modular elements (page 1, lines 1-17) whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements (page 9, lines 20-29). At least one of the modular elements individually protected by a cryptographic security code is a digital coupon (page 9, lines 29-32)

A server computer processes the order acceptance request (16) (page 5, lines 19-30) based on pre-programmed criteria, including authentication of the cryptographic security codes embedded within each of the modular elements (page 9, lines 6-29) and examination of the modular elements of the discrete message individually protected by the cryptographic security codes (page 5, line 18 - page 6, line 2), and, based on the processing of the order acceptance request (16), to transmit to the client computer an order acceptance response (18) based on the pre-programmed criteria (page 6, lines 3-24). The order acceptance response (18) comprises a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements (page 15, lines 16-25) whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements (page 10, lines 3-8; page 5, line 18 - page 6, line 2; page 21, lines 13-16). The server computer is programmed to determine whether a coupon holder is authorized to use the digital coupon and to accept the digital coupon only if the coupon holder is authorized to use the digital coupon (page 19, lines 16-29).

Independent claims 34 and 61 are directed to a client computer (12) being programmed to transmit to a server computer (14), over a public packet-switched network (FIG. 1), an order acceptance request (16) comprising a plurality of terms or conditions of a proposed offer for a purchase (specification page 1, lines 1-27). The order acceptance request comprises a discrete message that includes a plurality of modular elements (page 1, lines 1-17) whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements (page 9, lines 20-29). At least one of the modular elements individually protected by a cryptographic security code is a digital coupon (page 9, lines 29-32)

A server computer processes the order acceptance request (16) (page 5, lines 19-30) based on pre-programmed criteria, including authentication of the cryptographic security codes embedded within each of the modular elements (page 9, lines 6-29) and examination of the modular elements of the discrete message individually protected by the cryptographic security codes (page 5, line 18 - page 6, line 2), and, based on the processing of the order acceptance request (16), to transmit to the client computer an order acceptance response (18) based on the pre-programmed criteria (page 6, lines 3-24). The order acceptance response (18) comprises a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements (page 15, lines 16-25) whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements (page 10, lines 3-8; page 5, line 18 - page 6, line 2; page 21, lines13-16). The cryptographic security codes are embedded within respective ones of the plurality of modular elements (page 9, lines 20-23).

Independent claims 35 and 62 are directed to a client computer (12) being programmed to transmit to a server computer (14), over a public packet-switched network (FIG. 1), an order acceptance request (16) comprising a plurality of terms or conditions of a proposed offer for a purchase (specification page 1, lines 1-27). The order acceptance request comprises a discrete message that includes a plurality of modular elements (page 1, lines 1-17) whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements (page 9, lines 20-29). At least one of the modular elements individually protected by a cryptographic security code is a digital coupon (page 9, lines 29-32)

A server computer processes the order acceptance request (16) (page 5, lines 19-30) based on pre-programmed criteria, including authentication of the cryptographic security codes embedded within each of the modular elements (page 9, lines 6-29) and examination of the modular elements of the discrete message individually protected by the cryptographic security codes (page 5, line 18 - page 6, line 2), and, based on the processing of the order acceptance request (16), to transmit to the client computer an order acceptance response (18) based on the pre-programmed criteria (page 6, lines 3-24). The order acceptance response (18) comprises a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements (page 15, lines 16-25) whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements (page 10, lines 3-8; page 5, line 18 - page 6, line 2; page 21, lines13-16).

Independent claims 36 and 63 are directed to a client computer (12) being programmed to transmit to a server computer (14), over a public packet-switched network (FIG. 1), an order acceptance request (16) comprising a plurality of terms or conditions of a proposed offer for a purchase (specification page 1, lines 1-27). The order acceptance request comprises a discrete message that includes a plurality of modular elements (page 1, lines 1-17) whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements (page 9, lines 20-29). At least one of the modular elements individually protected by a cryptographic security code is a digital coupon (page 9, lines 29-32). The cryptographic security codes are digital signatures (page 9, lines 24-25).

A server computer processes the order acceptance request (16) (page 5, lines 19-30) based on pre-programmed criteria, including authentication of the cryptographic security codes embedded within each of the modular elements (page 9, lines 6-29) and examination of the modular elements of the discrete message individually protected by the cryptographic security codes (page 5, line 18 - page 6, line 2), and, based on the processing of the order acceptance request (16), to transmit to the client computer an order acceptance response (18) based on the pre-programmed criteria (page 6, lines 3-24). The order acceptance response (18) comprises a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements (page 15, lines 16-25) whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements (page 10, lines 3-8; page 5, line 18 - page 6, line 2; page 21, lines13-16).

B. THE REJECTION TO CLAIMS 12-36, 39-63 UNDER 35 U.S.C. §102(e) SHOULD BE REVERSED, BECAUSE THE *BARNETT* REFERENCE FAILS TO DISCLOSE MULTIPLE FEATURES RECITED IN CLAIMS.

Specifically, *Barnett* does not disclose a client computer configured for, or the step of, transmitting an order acceptance request over a packet-switched network that includes a plurality of modular elements, with each modular element individually protected by an embedded cryptographic security code, as recited in claims 12-14, 34-36, 39-41 and 61-63. Also among the features of the pending claims is a server configured to, or the step of, transmitting an order acceptance response to a client, the order acceptance response also including a plurality of modular elements whose individual integrity is protected by embedding a cryptographic security code within each modular element.

Barnett discloses a method and system for the electronic distribution of product redemption coupons to remote personal computers located at users' homes. A web site stores packages of coupon data for downloading on demand to the user's computer, where the user may view, select, sort and print desired coupons from the downloaded package (see Abstract, col. 4, lines 40-60). The user's demographic as well as coupon selection data is then provided back to the web site and coupon distributor and issuers for subsequent marketing analysis and the distributors/issuers can also determine how many times a particular coupon was viewed or downloaded (col. 5, lines 22-33).

When obtaining coupons under *Barnett*, a remote personal computer 6 is connected to a printer 8, that is instructed by the coupon data management routines 32 stored in the computer 6 in order to print coupons 18. Once printed, the coupons 18 are used in a conventional fashion by a consumer when shopping at a desired retail store 10. In other words, the coupons 18 are physically presented in a paper form to a product checkout station 11 along with the associated products for purchase, and the discount amount shown on the coupon 18 is credited to the consumer at the point of sale (col. 7, lines 6-17). According to *Barnett*, the coupons 18 contain user-specific data in the form of a unique user bar code 90, as shown graphically in FIG. 5. The user bar code 90 is encoded with user-specific information such as the user name and/or other unique identification criteria such as a social security number or online service address (col. 7, lines 21-35).

Thus, *Barnett* teaches a central server that (1) collects information and identification from users accessing the server requesting coupons, (2) encodes user and product information into a barcode, (3) formats the barcode and other text/graphics into the form of a printable coupon, and (4) transmits the printable coupon over the network to the user for subsequent printing and redemption (col. 4, lines 40-60; col. 5, lines 22-33; col. 7, lines 6-17, 21-25).

In the Office Action, and during the Examiner Interview conducted August 31, 2006, it was stated by the Examiner that the process of "encoding" data into a printable barcode format to create a "virtually fraud-proof" coupon was the equivalent of cryptographic encoding. This is simply incorrect and misstates the teaching of the underlying technology. Bar-coding, such as the type recited in *Barnett*, is premised upon *symbology*, which deals with encoding digits/characters of a message, as well as the start and stop markers, into bars and space. The symbology of the barcode (e.g., UPC code) is merely a machine-readable representation of information in a visual format on the physical surface of a coupon (such as ref. 90 of *Barnett*). There is no encryption or ciphering of the data whatsoever; it is merely converted into a format that can be read quickly and easily by a fixed-light or laser scanner, instead of being manually read by a merchant. The Office Actions have failed to identify what teaching in *Barnett* discloses in the barcode a plurality of modular elements whose individual integrity is protected by embedding a cryptographic security code within each modular element. Under the barcode conversion of Barnett, *all of the coupon information is jointly translated into a singular barcode* (col. 7, lines 22-35).

Furthermore, the references in *Barnett* to the coupon being "virtually fraud-proof" has nothing to do with the integrity of the data being transmitted over the network. Instead, *Barnett* provides and stores unique identity information to each coupon (e.g., user information, expiration date), where the coupon redemption center may control the time (i.e., before an expiration date) or manner (i.e., only one coupon redemption per user) in which the coupon is redeemed based on this identity information (see col. 11, lines 2-23). The "fraud" referred in Barnett deals with instances where (1) photocopies are made of coupons in an effort to obtain multiple redemptions (col. 11, lines 11-23), or (2) someone other than the user (who presumably can't provide identification to the merchant at the time of redemption) is attempting to redeem a prohibited coupon (col. 7, lines 21-34). None of this has anything to do with cryptographic protection and also has no relation whatsoever to transactions being performed over a public packet-switched network.

In contrast to *Barnett*, the present claims rely on *cryptography* in the form of security codes embedded within each of the plurality of modular elements, where at least one of the modular elements individually protected by a cryptographic security code is a digital coupon. As is known in the art, cryptography deals with the secure encoding and authentication of the data itself. Appellants note that each of the above claims recite the "authentication of the cryptographic security codes embedded within each of the modular elements." As described above, the present specification describes, as an example, the use of key authentication, such as SSL, which contain cryptographic protocols which provide secure communications on the Internet (page 9, lines 6-29; see also page 19, lines 21-28). Under the example of SSL, only the server is authenticated (i.e. its identity is ensured) while the client remains unauthenticated. For mutual authentication, clients must be provided with public key infrastructure (PKI) deployment. The protocols allow client/server applications to communicate in a way designed to prevent eavesdropping, tampering, and message forgery during the transmission and recept of a commercial transaction that occurs over the Internet. Claims 35 and 62 specifically recite the use of digital signatures, and claims 36 and 63 specifically recite the use of message authentication codes.

None of this is either taught or suggested in *Barnett* – as discussed above, *Barnett's* system does not conduct commercial transactions over the Internet using the coupons; the entire disclosure is premised entirely on the user printing and physically redeeming the coupon at a retail store or coupon redemption center through the use of barcode scanning. *Barnett* briefly mentions that coupons may be redeemed "electronically" (see FIG. 9, col. 11, lines 29-42), however, it is clear from the disclosure that the "electronic" redeeming of coupons involves the transmission and storage of the coupon at the retail center, where the retail center prints and scans the coupon on location ("[t]hus, the printable coupon data generation routine ***32d*** combines all this information and generates a record indicative of the unique coupon to be printed"). Cryptographic encoding has no application under the teaching of *Barnett*. Since the coupons are physically printed and scanned, use of PKI certificates would have no bearing on the alleged "fraud proof" nature of the coupons, the entire purpose of such coding would be lost upon subsequent barcoding and printing of the user information.

As *Barnett* does not conduct transactions of the products underlying the printed coupons, *Barnett* also fails to teach or suggest the processing and negotiatiation of electronically authenticated coupons. The present claims recite that the order acceptance request is authenticated and processed to contain a discreet message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements. *Barnett* is completely silent as to how each of the user information is individually protected through the use of barcodes.

Also, claims 12 and 39 recite that the client computer is programmed to receive the digital coupon, protected by a cryptographic security code, "from another computer." During the Examiner interview, it was posited by the examiner that the term "another computer" was broad, and that, using a commensurately and "reasonably" broad interpretation, "another computer" was being interpreted as the "server computer." Appellants respectfully submit that this interpretation is simply wrong and contradicts every convention of claim interpretation. "Another computer" should mean simply that - a computer that is neither the client computer nor the server computer. An exemplary disclosure of this interpretation may be found in the specification on page 9, lines 29-32. *Barnett* clearly does not disclose this configuration, as the entire teaching is premised on providing barcoded coupons from the same central server (see Abstract, col. 4, lines 40-52).

Furthermore, claims 13 and 40 further recite that the authenticated coupons are accepted "without regard to the identity of the coupon holder." These elements are clearly not taught or suggested in the disclosure of *Barnett*. As was explained to the Examiner during the Interview, *Barnett* states that the identification of the user is required to make each coupon "unique" and to provide added security for each issued coupon (col. 7, lines 21-31). Thus, *Barnett* clearly fails to disclose the claimed features.

It is mandated that the USPTO determines the scope of claims in patent applications not solely on the basis of the claim language, but upon giving claims their broadest reasonable construction "in light of the specification as it would be interpreted by one of ordinary skill in the art." *In re Am. Acad. of Sci. Tech. Ctr.*, 367 F.3d 1359, 1364 (Fed. Cir. 2004). Indeed, the rules of the PTO require that application claims must "conform to the invention as set forth in the remainder of the specification and the terms and phrases used in the claims must find clear support or antecedent basis in the description so that the meaning of the terms in the claims may be ascertainable by reference to the description." 37 CFR 1.75(d)(1) (MPEP 2111). The broadest reasonable interpretation of the claims must also be consistent with the interpretation that those skilled in the art would reach. *In re Cortright*, 165 F.3d 1353, 1359 (Fed. Cir. 1999).

Appellants respectfully submit that, not only is the Examiner misinterpreting the scope and content of the prior art, but is also applying a claim interpretation to the present application that is inconsistent with the express claim language, and clearly contrary to well-understood technical terms of art (i.e., "cryptographic security codes").

E. THE PATENTABILITY OF CLAIMS 12-14, 34-36, 39-41 AND 61-63 RENDERS MOOT THE REJECTIONS OF CLAIMS 15-33, AND 42-60

Dependent Claims 15-33 and 42-60 were also rejected under 35 U.S.C. §102(e) as being unpatentable over *Barnett et al.* (US Patent 6,321,208). Appellants respectfully submit that the patentability of independent Claims 12-14, 34-36, 39-41 and 61-63 as previously discussed renders moot the obviousness rejections of Claims 15-33 and 42-60. In this regard, the cited art fails to teach or suggest the elements of these claims in direct/indirect combination with their respective independent claims.

VIII. CONCLUSION

Appellants respectfully submit that Claims 12-36 and 39-63 are novel and non-obvious in view of the cited references for the reasons previously discussed. Accordingly, Appellants respectfully submit that the rejections under 35 U.S.C. §102(e) are erroneous in law and in fact and should therefore be reversed by this Board.

The Director is authorized to charge $500 for the Appeal Brief and any additional fees which may be required, or to credit any overpayment to Deposit Account No. 02-1818. If such a withdrawal is made, please indicate the Attorney Docket No. 115274-008 on the account statement.

Respectfully submitted,

BELL, BOYD & LLOYD LLC

BY ____________________
Peter Zura
Reg. No. 48,196
Customer No.: 24573
Phone: (312) 807-4208

Dated: April 16, 2007

CLAIMS APPENDIX

PENDING CLAIMS ON APPEAL OF U.S. PATENT APPLICATION SERIAL NO. 09/054,180

Claims 1-11 (canceled).

Claim 12 (previously presented): An electronic commerce system comprising:

a client computer; and

a server computer;

the client computer and the server computer being interconnected by a public packet switched communications network;

the client computer being programmed to transmit to the server computer an order acceptance request comprising a plurality of terms or conditions of a proposed offer for a purchase, the order acceptance request comprising a discrete message that includes a plurality of modular elements whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements, at least one of the modular elements individually protected by a cryptographic security code being a digital coupon;

the server computer being programmed to process the order acceptance request based on pre-programmed criteria, including authentication of the cryptographic security codes embedded within each of the modular elements and examination of the modular elements of the discrete message individually protected by the cryptographic security codes, and, based on the processing of the order acceptance request, to transmit to the client computer an order acceptance response based on the pre-programmed criteria, the order acceptance response comprising a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements;

wherein the client computer is programmed to receive the digital coupon, protected by a cryptographic security code, from another computer.

Claim 13 (previously presented): An electronic commerce system comprising:

a client computer; and

a server computer;

the client computer and the server computer being interconnected by a public packet switched communications network;

the client computer being programmed to transmit to the server computer an order acceptance request comprising a plurality of terms or conditions of a proposed offer for a purchase, the order acceptance request comprising a discrete message that includes a plurality of modular elements whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements, at least one of the modular elements individually protected by a cryptographic security code being a digital coupon;

the server computer being programmed to process the order acceptance request based on pre-programmed criteria, including authentication of the cryptographic security codes embedded within each of the modular elements and examination of the modular elements of the discrete message individually protected by the cryptographic security codes, and, based on the processing of the order acceptance request, to transmit to the client computer an order acceptance response based on the pre-programmed criteria, the order acceptance response comprising a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements;

wherein the digital coupon is configured to be used by any coupon holder that possesses the digital coupon, and wherein the server computer is programmed to accept the digital coupon without regard to the identity of the coupon holder.

Claim 14 (previously presented): An electronic commerce system comprising:

a client computer; and

a server computer;

the client computer and the server computer being interconnected by a public packet switched communications network;

the client computer being programmed to transmit to the server computer an order acceptance request comprising a plurality of terms or conditions of a proposed offer for a purchase, the order acceptance request comprising a discrete message that includes a plurality of modular elements whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements, at least one of the modular elements individually protected by a cryptographic security code being a digital coupon;

the server computer being programmed to process the order acceptance request based on pre-programmed criteria, including authentication of the cryptographic security codes embedded within each of the modular elements and examination of the modular elements of the discrete message individually protected by the cryptographic security codes, and, based on the processing of the order acceptance request, to transmit to the client computer an order acceptance response based on the pre-programmed criteria, the order acceptance response comprising a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements;

wherein the server computer is programmed to determine whether a coupon holder is authorized to use the digital coupon and to accept the digital coupon only if the coupon holder is authorized to use the digital coupon.

Claim 15 (previously presented): The electronic commerce system of claim 14 wherein the client computer is programmed to provide information to the server computer concerning identify of the coupon holder.

Claim 16 (previously presented): The electronic commerce system of claim 15 wherein the server computer is programmed to authenticate authority of the client computer by virtue of a two-way-authenticated SSL connection.

Claim 17 (previously presented): The electronic commerce system of claim 15 wherein the server computer is programmed to authenticate authority of the client computer using a basic authentication method.

Claim 18 (previously presented): The electronic commerce system of claim 15 wherein the server computer is programmed to authenticate authority of the client computer using a client certificate.

Claim 19 (previously presented): The electronic commerce system of claim 3 wherein the digital coupon contains a serial number to ensure that the digital coupon is used only once and the server computer is programmed to determine whether the digital coupon has been used previously and to accept the digital coupon only if it has not been used previously.

Claim 20 (previously presented): The electronic commerce system of claim 3 wherein the server computer is programmed to set at least one term of the order acceptance response based on whether the digital coupon is present in the order acceptance request.

Claim 21 (previously presented): The electronic commerce system of claim 20 wherein the at least one term of the order acceptance response is a price.

Claim 22 (previously presented): The electronic commerce system of claim 3 wherein the server computer is programmed to set at least one term of the order acceptance response based on whether the digital coupon in the order acceptance request is a particular type of digital coupon.

Claim 23 (previously presented): The electronic commerce system of claim 3 wherein the digital coupon is a gift certificate.

Claim 24 (previously presented): The electronic commerce system of claim 23 wherein the gift certificate comprises a serial number.

Claim 25 (previously presented): The electronic commerce system of claim 24 wherein the server computer is programmed to ensure that the serial number has been used only once by checking a database in which the serial number is stored.

Claim 26 (previously presented): The electronic commerce system of claim 23 wherein the client computer is programmed to display an icon of the gift certificate and to initiate the order acceptance request after a recipient of the gift certificate clicks on the icon.

Claim 27 (previously presented): The electronic commerce system of claim 26 further comprising a merchant computer, the merchant computer being programmed to respond to the recipient clicking on the icon by transmitting an order form to the client computer, the client computer being programmed to initiate the order acceptance request when the recipient fills in the order form.

Claim 28 (previously presented): The electronic commerce system of claim 23 wherein the client computer is a first client computer programmed to receive the gift certificate from a second client computer.

Claim 29 (previously presented): The electronic commerce system of claim 28 wherein the server computer is programmed to transmit the gift certificate to the second client computer, which in turn is programmed to forward the gift certificate to the first client computer.

Claim 30 (previously presented): The electronic commerce system of claim 29 wherein the gift certificate comprises a serial number and the server computer is programmed to create the serial number of the gift certificate before transmitting the gift certificate to the second client computer.

Claim 31 (previously presented): The electronic commerce system of claim 30 wherein the server computer is programmed to store the serial number in a database before transmitting the gift certificate to the second client computer, and is programmed, when it receives the gift certificate from the first client computer to ensure that the serial number has been used only once by checking the database in which the serial number is stored.

Claim 32 (previously presented): The electronic commerce system of claim 29 further comprising a merchant computer programmed to transmit the gift certificate to the server computer before the server computer transmits the gift certificate to the second client computer.

Claim 33 (previously presented): The electronic commerce system of claim 32 wherein the merchant computer is programmed to transmit the gift certificate to the server computer in the form of an order acceptance request that includes extension information indicating that the order acceptance request is a gift certificate.

Claim 34 (previously presented): An electronic commerce system comprising:

a client computer; and

a server computer;

the client computer and the server computer being interconnected by a public packet switched communications network;

the client computer being programmed to transmit to the server computer an order acceptance request comprising a plurality of terms or conditions of a proposed offer for a purchase, the order acceptance request comprising a discrete message that includes a plurality of modular elements whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements, at least one of the modular elements individually protected by a cryptographic security code being a digital coupon;

the server computer being programmed to process the order acceptance request based on pre-programmed criteria, including authentication of the cryptographic security codes embedded within each of the modular elements and examination of the modular elements of the discrete message individually protected by the cryptographic security codes, and, based on the processing of the order acceptance request, to transmit to the client computer an order acceptance response based on the pre-programmed criteria, the order acceptance response comprising a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements;

wherein the cryptographic security codes are embedded within respective ones of the plurality of modular elements.

Claim 35 (previously presented): An electronic commerce system comprising:

a client computer; and

a server computer;

the client computer and the server computer being interconnected by a public packet switched communications network;

the client computer being programmed to transmit to the server computer an order acceptance request comprising a plurality of terms or conditions of a proposed offer for a purchase, the order acceptance request comprising a discrete message that includes a plurality of modular elements whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements, at least one of the modular elements individually protected by a cryptographic security code being a digital coupon;

the server computer being programmed to process the order acceptance request based on pre-programmed criteria, including authentication of the cryptographic security codes embedded within each of the modular elements and examination of the modular elements of the discrete message individually protected by the cryptographic security codes, and, based on the processing of the order acceptance request, to transmit to the client computer an order acceptance response based on the pre-programmed criteria, the order acceptance response comprising a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements;

wherein the cryptographic security codes are digital signatures.

Claim 36 (previously presented): An electronic commerce system comprising:

a client computer; and

a server computer;

the client computer and the server computer being interconnected by a public packet switched communications network;

the client computer being programmed to transmit to the server computer an order acceptance request comprising a plurality of terms or conditions of a proposed offer for a purchase, the order acceptance request comprising a discrete message that includes a plurality of modular elements whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements, at least one of the modular elements individually protected by a cryptographic security code being a digital coupon;

the server computer being programmed to process the order acceptance request based on pre-programmed criteria, including authentication of the cryptographic security codes embedded within each of the modular elements and examination of the modular elements of the discrete message individually protected by the cryptographic security codes, and, based on the processing of the order acceptance request, to transmit to the client computer an order acceptance response based on the pre-programmed criteria, the order acceptance response comprising a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements;

wherein the cryptographic security codes are message authentication codes.

Claims 37-38 (canceled).

Claim 39 (previously presented): A method of processing order acceptance requests in an electronic commerce system, comprising a client computer and a server computer interconnected by a public packet switched communications network, the method comprising:

receiving at the server computer an order acceptance request transmitted by the client computer comprising a plurality of terms or conditions of a proposed offer for a purchase, the order acceptance request comprising a discrete message that includes a plurality of modular elements whose individual integrity is protected by cryptographic security codes embedded within each of the modular elements, at least one of the modular elements individually protected by a cryptographic security code being a digital coupon;

processing the order acceptance request based on pre-programmed criteria, including authentication of the cryptographic security codes and examination of the modular elements of the discrete message individually protected by the cryptographic security codes; and

based on the processing of the order acceptance request, transmitting to the client computer an order acceptance response based on the pre-programmed criteria, the order acceptance response comprising a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements whose individual integrity is protected by cryptographic security codes embedded within each of the modular elements;

wherein the client computer receives the digital coupon, protected by a cryptographic security code, from another computer.

Claim 40 (previously presented): A method of processing order acceptance requests in an electronic commerce system, comprising a client computer and a server computer interconnected by a public packet switched communications network, the method comprising:

receiving at the server computer an order acceptance request transmitted by the client computer comprising a plurality of terms or conditions of a proposed offer for a purchase, the order acceptance request comprising a discrete message that includes a plurality of modular elements whose individual integrity is protected by cryptographic security codes embedded within each of the modular elements, at least one of the modular elements individually protected by a cryptographic security code being a digital coupon;

processing the order acceptance request based on pre-programmed criteria, including authentication of the cryptographic security codes and examination of the modular elements of the discrete message individually protected by the cryptographic security codes; and

based on the processing of the order acceptance request, transmitting to the client computer an order acceptance response based on the pre-programmed criteria, the order acceptance response comprising a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements whose individual integrity is protected by cryptographic security codes embedded within each of the modular elements;

wherein the digital coupon is configured to be used by any coupon holder that possesses the digital coupon, the method further comprising accepting the digital coupon at the server computer is programmed without regard to identity to the coupon holder.

Claim 41 (previously presented): A method of processing order acceptance requests in an electronic commerce system, comprising a client computer and a server computer interconnected by a public packet switched communications network, the method comprising:

receiving at the server computer an order acceptance request transmitted by the client computer comprising a plurality of terms or conditions of a proposed offer for a purchase, the order acceptance request comprising a discrete message that includes a plurality of modular elements whose individual integrity is protected by cryptographic security codes embedded within each of the modular elements, at least one of the modular elements individually protected by a cryptographic security code being a digital coupon;

processing the order acceptance request based on pre-programmed criteria, including authentication of the cryptographic security codes and examination of the modular elements of the discrete message individually protected by the cryptographic security codes; and

based on the processing of the order acceptance request, transmitting to the client computer an order acceptance response based on the pre-programmed criteria, the order acceptance response comprising a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements whose individual integrity is protected by cryptographic security codes embedded within each of the modular elements;

further comprising the steps of determining whether a coupon holder is authorized to use the digital coupon and accepting the digital coupon at the server computer only if the coupon holder is authorized to use the digital coupon.

Claim 42 (previously presented): The method of claim 41 further comprising receiving information at the server computer provided by the client computer concerning identify of the coupon holder.

Claim 43 (previously presented): The method of claim 42 further comprising authenticating authority of the client computer, at the server computer, by virtue of a two-way-authenticated SSL connection.

Claim 44 (previously presented): The method of claim 42 wherein authenticating authority of the client computer is performed using a basic authentication method.

Claim 45 (previously presented): The method of claim 42 wherein authenticating authority of the client computer is performed using a client certificate.

Claim 46 (previously presented): The method of claim 37 wherein the digital coupon contains a serial number to ensure that the digital coupon is used only once, the method further comprising determining at the server computer whether the digital coupon has been used previously and accepting the digital coupon only if it has not been used previously.

Claim 47 (previously presented): The method of claim 37 further comprising setting, at the server computer, at least one term of the order acceptance response based on whether the digital coupon is present in the order acceptance request.

Claim 48 (previously presented): The method of claim 47 wherein the at least one term of the order acceptance response is a price.

Claim 49 (previously presented): The method of claim 37 further comprising setting, at the server computer, at least one term of the order acceptance response based on whether the digital coupon in the order acceptance request is a particular type of digital coupon.

Claim 50 (previously presented): The method of claim 37 wherein the digital coupon is a gift certificate.

Claim 51 (previously presented): The method of claim 50 wherein the gift certificate comprises a serial number.

Claim 52 (previously presented): The method of claim 51 further comprising ensuring that the serial number has been used only once by checking a database at the server computer in which the serial number is stored.

Claim 53 (previously presented): The method of claim 50 wherein the client computer displays an icon of the gift certificate and initiates the order acceptance request after a recipient of the gift certificate clicks on the icon.

Claim 54 (previously presented): The method of claim 53 wherein the electronic commerce system further comprises a merchant computer and wherein the merchant computer responds to the recipient clicking on the icon by transmitting an order form to the client computer, and wherein the client computer initiates the order acceptance request when the recipient fills in the order form.

Claim 55 (previously presented): The method of claim 50 wherein the client computer is a first client computer that receive the gift certificate from a second client computer in the electronic commerce system.

Claim 56 (previously presented): The method of claim 55 further comprising transmitting the gift certificate from the server computer to the second client computer, which in turn forwards the gift certificate to the first client computer.

Claim 57 (previously presented): The method of claim 56 wherein the gift certificate comprises a serial number and wherein the method further comprises creating the serial number of the gift certificate at the server computer before transmitting the gift certificate to the second client computer.

Claim 58 (previously presented): The method of claim 56 further comprising storing the serial number in a database at the server computer before transmitting the gift certificate to the second client computer, and when the server computer receives the gift certificate from the first client computer, ensuring that the serial number has been used only once by checking the database at the server computer in which the serial number is stored.

Claim 59 (previously presented): The method of claim 56 further wherein the electronic commerce system further comprises a merchant computer, the method further comprising receiving the gift certificate at the server computer from the merchant computer before transmitting the gift certificate from the server computer to the second client computer.

Claim 60 (previously presented): The method of claim 59 wherein the merchant computer transmits the gift certificate to the server computer in the form of an order acceptance request that includes extension information indicating that the order acceptance request is a gift certificate.

Claim 61 (previously presented): A method of processing order acceptance requests in an electronic commerce system, comprising a client computer and a server computer interconnected by a public packet switched communications network, the method comprising:

receiving at the server computer an order acceptance request transmitted by the client computer comprising a plurality of terms or conditions of a proposed offer for a purchase, the order acceptance request comprising a discrete message that includes a plurality of modular elements whose individual integrity is protected by cryptographic security codes embedded within each of the modular elements, at least one of the modular elements individually protected by a cryptographic security code being a digital coupon;

processing the order acceptance request based on pre-programmed criteria, including authentication of the cryptographic security codes and examination of the modular elements of the discrete message individually protected by the cryptographic security codes; and

based on the processing of the order acceptance request, transmitting to the client computer an order acceptance response based on the pre-programmed criteria, the order acceptance response comprising a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements whose individual integrity is protected by cryptographic security codes embedded within each of the modular elements;

wherein the cryptographic security codes are embedded within respective ones of the plurality of modular elements.

Claim 62 (previously presented): A method of processing order acceptance requests in an electronic commerce system, comprising a client computer and a server computer interconnected by a public packet switched communications network, the method comprising:

receiving at the server computer an order acceptance request transmitted by the client computer comprising a plurality of terms or conditions of a proposed offer for a purchase, the order acceptance request comprising a discrete message that includes a plurality of modular elements whose individual integrity is protected by cryptographic security codes embedded within each of the modular elements, at least one of the modular elements individually protected by a cryptographic security code being a digital coupon;

processing the order acceptance request based on pre-programmed criteria, including authentication of the cryptographic security codes and examination of the modular elements of the discrete message individually protected by the cryptographic security codes; and

based on the processing of the order acceptance request, transmitting to the client computer an order acceptance response based on the pre-programmed criteria, the order acceptance response comprising a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements whose individual integrity is protected by cryptographic security codes embedded within each of the modular elements;

wherein the cryptographic security codes are digital signatures.

Claim 63 (previously presented): A method of processing order acceptance requests in an electronic commerce system, comprising a client computer and a server computer interconnected by a public packet switched communications network, the method comprising:

receiving at the server computer an order acceptance request transmitted by the client computer comprising a plurality of terms or conditions of a proposed offer for a purchase, the order acceptance request comprising a discrete message that includes a plurality of modular elements whose individual integrity is protected by cryptographic security codes embedded within each of the modular elements, at least one of the modular elements individually protected by a cryptographic security code being a digital coupon;

processing the order acceptance request based on pre-programmed criteria, including authentication of the cryptographic security codes and examination of the modular elements of the discrete message individually protected by the cryptographic security codes; and

based on the processing of the order acceptance request, transmitting to the client computer an order acceptance response based on the pre-programmed criteria, the order acceptance response comprising a discrete message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements whose individual integrity is protected by cryptographic security codes embedded within each of the modular elements;

wherein the cryptographic security codes are message authentication codes.

EVIDENCE APPENDIX

EXHIBIT A: Final Office Action dated June 14, 2006.

EXHIBIT B: *Barnett et al.* (US Patent 6,321,208) cited by the Examiner in the Office Action dated June 14, 2006.

RELATED PROCEEDINGS APPENDIX

None

APPENDIX A

Final Office Action dated June 14, 2006

[*Submitted with Appeal Brief filed December 18, 2006*]

APPENDIX B

Barnett et al. (US Patent 6,321,208) cited by the Examiner in the Office Action dated June 14, 2006.

[*Submitted with Appeal Brief filed December 18, 2006*]